

Get started with Compliance Manager

<https://docs.microsoft.com/en-us/microsoft-365/compliance/compliance-manager-setup?view=o365-worldwide>

Get started with Compliance Manager

Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded. For more information about Microsoft Purview, see the [blog announcement](#).

In this article: This article helps you set up Compliance Manager. Learn how to **access** Compliance Manager, **set roles and permissions**, and configure **automatic testing of improvement actions**. Walk through **your Compliance Manager dashboard** and understand the main pages: the improvement actions page, the solutions page, the assessments page, and the assessment templates page.

Who can access Compliance Manager

Compliance Manager is available to organizations with Office 365 and Microsoft 365 licenses, and to US Government Community Cloud (GCC) Moderate, GCC High, and Department of Defense (DoD) customers. Assessment availability and management capabilities depend on your licensing agreement. [View service description details](#).

Before you begin

The Microsoft 365 global administrator for your organization will likely be the first user to access Compliance Manager. We recommend the global admin sign in and set user permissions as outlined below when visiting Compliance Manager for the first time.

Sign in

1. Go to the [Microsoft Purview compliance portal](#) and **sign in** with your Microsoft 365 global administrator account.
2. Select **Compliance Manager** on the left navigation pane. You'll arrive at your [Compliance Manager dashboard](#).

The direct link to access Compliance Manager is <https://compliance.microsoft.com/compliancemanager>.

Set user permissions and assign roles

Compliance Manager uses a role-based access control (RBAC) permission model. Only users who are assigned a role may access Compliance Manager, and the actions allowed by each user are restricted by [role type](#).

Where to set permissions

The person holding the [global admin role](#) for your organization can set user permissions for Compliance Manager. Permissions can be set in the Microsoft Purview compliance portal as well as in Azure Active Directory (Azure AD).

Note

Customers in US Government Community (GCC) High and Department of Defense (DoD) environments can only set user permissions and roles for Compliance Manager in Azure AD. See below for Azure AD instructions and role type definitions.

To set permissions and assign roles in the Microsoft Purview compliance portal, follow the steps below:

1. Go to the Microsoft Purview compliance portal, and select [Permissions](#).
2. Under the compliance portal dropdown, select **Roles**.
3. Find the role group to which you want to add one or more users, and check the box to the left of the group name. (See the [list of roles and related functions below](#). The role group names mimic the role name.)
4. On the flyout pane for that group, select **Edit** under the **Members** header.
5. Select **Choose members**. Another flyout window will appear.
6. Select **+ Add** to choose one or more users to add to the group.

7. Select the checkbox next to the names you want to add, then select the **Add** button at the bottom.
8. When you're done assigning users, select **Done**, then select **Save**, then **Close**.

More about Azure AD

To assign roles and set permissions in Azure AD, see [Assign administrator and non-administrator roles to users with Azure Active Directory](#).

Users with Azure AD identities who don't have Office 365 or Microsoft 365 subscriptions won't be able to access Compliance Manager in the Microsoft Purview compliance portal. To seek assistance in accessing Compliance Manager, contact cmresearch@microsoft.com.

Role types

The table below shows the functions allowed by each role in Compliance Manager. The table also shows how each [Azure AD role](#) maps to Compliance Manager roles. Users will need at least the Compliance Manager reader role, or Azure AD global reader role, to access Compliance Manager.

User can:	Compliance Manager role	Azure AD role
Read but not edit data	Compliance Manager Reader	Azure AD Global reader, Security reader
Edit data	Compliance Manager Contribution	Compliance Administrator
Edit test results	Compliance Manager Assessor	Compliance Administrator

User can:	Compliance Manager role	Azure AD role
Manage assessments, and template and tenant data	Compliance Manager Administration	Compliance Administrator, Compliance Data Administrator, Security Administrator
Assign users	Global Administrator	Global Administrator

Start a premium assessments trial

The Compliance Manager premium assessments trial is a great way to quickly set up assessments that are most relevant to your organization. Our library of over 300 templates correspond to governmental regulations and industry standards around the world. Learn more about the [premium assessments trial](#).

You can start your trial directly from Compliance Manager and set up recommended assessments by following these steps:

1. On the Compliance Manager **Overview** page, select **Start trial**. You'll enter a trial activation wizard which will ask questions to help us recommend assessments for your organization.
2. On the **Activate trial** page, select **Next** to begin your free 90 day premium assessments trial and continue with creating assessments.
3. Select one or more industries that identify your organization, then select **Next**.
4. Select one or more regions for your organization's location, then select **Next**.
5. On the **Choose assessments** screen, select the dropdown arrow next to **Recommended templates** to see the list of assessments we think apply to your organization. Check the boxes next to the templates you want to use for creating assessments, then select **Next**.
6. Review your final selections and select **Add Recommended Assessments** to create your new assessments.

Learn more about getting started with assessments by visiting the [Assessments page](#) section below.

Settings for automated testing and user history

The Compliance Manager settings in the Microsoft Purview compliance portal allow you to enable and disable automatic testing of improvement actions. The settings also allow

you to manage the data of users associated to improvement actions, including the ability to reassign improvement actions to a different user. Only people with a global administrator or Compliance Manager Administrator role can access the Compliance Manager settings.

Note

The automated testing feature is not available to customers in GCC High and DoD environments because Secure Score isn't available in these environments. GCC High and DoD customers will need to manually implement and test their improvement actions.

Set up automated testing

Compliance Manager detects signals from other Microsoft Purview solutions that your organization subscribes to, including data lifecycle management, information protection, Microsoft Purview Data Loss Prevention, communication compliance, and insider risk management. In each improvement action's details page, the **Testing logic** field on the **Testing** tab will show what's required in the other solution in order for the action to pass and earn points toward your compliance score.

Compliance Manager also detects signals from complementary improvement actions that are also monitored by [Microsoft Secure Score](#). Using these signals, Compliance Manager can automatically test certain improvement actions for you, which helps maximize efficiency in your compliance activities. When an improvement action is successfully tested and implemented, you receive the full amount of points, which gets credited to your overall compliance score.

Automatic testing is turned on by default for organizations new to Compliance Manager. When you first deploy Microsoft 365 or Office 365, it takes approximately seven days to fully collect data and factor it into your compliance score. When automated testing is turned on, the action's test date won't be updated, but its test status will update. When new assessments are created, scores automatically include Microsoft control scores and Secure Score integration.

Manage automated testing settings

The global administrator for your organization can change the settings for automated testing at any time. You can turn off automated testing for

common improvement actions, or turn it on for individual actions. Follow the instructions below to change your automated testing settings.

1. Select **Settings** in the Microsoft Purview compliance portal.
2. On the settings page, select **Compliance Manager**.
3. Select **Testing source** from the left navigation.
4. Select the applicable button to turn on automatic testing for all improvement actions, turn it off for all actions, or turn on by individual action.
5. If you select **Turn on per improvement action**, a list will show all the available improvement actions to choose from. Check the box next to any action you want automatically tested.
6. Select **Save** to save your settings. You'll receive a confirmation message at the top of your screen that your selection was saved. If you receive a failure notice, try again.

Note: Only the global administrator can turn on or off automatic updates for all actions. The Compliance Manager Administrator can turn on automatic updates for individual actions, but not for all actions globally.

Learn more

- [Learn more about how continuous monitoring contributes to your compliance score.](#)
- [Learn more about designating a testing source for an improvement action.](#)

Manage user history

The **Manage user history** settings help you quickly identify which users have worked with improvement actions in Compliance Manager. The identifiable user data associated with improvement actions includes any implementation and testing work done,

documents they uploaded, and any notes they entered. Understanding and retrieving this type of data may be necessary for your organization's own compliance needs.

The user history settings also allow you to reassign all improvement actions from one user to another.

To find the user history settings:

1. Select **Settings** in the Microsoft Purview compliance portal.
2. On the settings page, select **Compliance Manager**.
3. Select **Manage user history** from the left navigation.

The **manage user history** page shows a list of all users by email address who are assigned to an improvement action. Use the **Search** button to quickly find a specific user by typing in their email address.

To the right of each user's email address, the **Select** drop-down menu provides options to export a report, reassign improvement actions, or delete history. See each section below for details about each option.

Export a report of user history data

You can export an Excel file containing a list of improvement actions currently assigned to a user. The report also lists any evidence files uploaded by that user. This information can help you reassign open improvement actions.

The report reflects the improvement action's status as of its creation date. It's not a historical report of all previous changes to its status or assignment (learn how to [export a report from your improvement actions page](#)).

Follow the steps below to export a report by user:

1. Select **Settings** in the Microsoft Purview compliance portal.

2. On the settings page, select **Compliance Manager**.
3. Select **Manage user history** from the navigation at left.
4. Find your intended user by searching the list email addresses, or by selecting **Search** and entering the user's email address.
5. From the **Select** drop-down menu, choose **Export report**.
6. Once the Excel file of your report is generated, you can open it and save it to your local machine.

Reassign improvement actions to another user

You can reassign improvement actions from one user to another. When you reassign an action, the document upload history doesn't change, but the name of the user who originally uploaded the documentation no longer appears within the improvement action.

Follow the steps below to reassign improvement actions to another user:

1. Select **Settings** in the Microsoft Purview compliance portal.
2. On the settings page, select **Compliance Manager**.
3. Select **Manage user history** from the navigation at left.
4. Find a user by searching the list email addresses, or by selecting **Search** and entering that user's email address.
5. From the **Select** drop-down menu, choose **Reassign improvement actions**. The **Reassign improvement actions** flyout pane will appear.
6. In the **Search users** field, enter the name or email address of the user you want assign the improvement actions to.

7. When you see the name of your intended user under **Improvement actions will be assigned to**, select the user, then select **Assign actions**.

8. When the reassignment is complete, you'll see a confirmation message in the flyout pane confirming that all improvement actions from the previous user have been reassigned to the new user. If you receive a reassignment failure notice, close the window and try again. To close the flyout pane, select **Done**.

The new assignee receives an email that they've been assigned to an improvement action. The email contains a direct link into the improvement action's details page.

Note

If you reassign an action that has a pending update, the direct link to the action in the reassignment email will break if the update is accepted after reassignment. You can fix this by re-assigning the action to the user after the update is accepted. Learn more about [updates to improvement actions](#).

Delete user history

Deleting a user's history will remove them as an owner of improvement actions, and will remove their name from all other fields in Compliance Manager. When you delete a user's history, the improvement actions they owned will not display an **Assigned to** value until a new user is assigned. Any documents uploaded to the improvement action will show **User removed** in place of the deleted user's name. Deleting user history is permanent.

To delete a user's history, follow the steps below:

1. Select **Settings** in the Microsoft Purview compliance portal.
2. On the settings page, select **Compliance Manager**.
3. Select **Manage user history** from the navigation at left.
4. Find a user by searching the list email addresses, or by selecting **Search** and entering that user's email address.
5. From the **Select** drop-down menu, choose **Delete history**.
6. A window appears asking you to confirm the permanent deletion of the user's history. To continue with deletion, select **Delete history**. To leave without deleting the history, select **Cancel**.
7. You'll arrive back at the **Manage user history** page with a confirmation message at the top that the history for the user was deleted.

Understand the Compliance Manager dashboard

The Compliance Manager dashboard is designed to provide you an at-a-glance view of your current compliance posture.



Home



Compliance Manager



Data classification



Data connectors



Alerts



Reports



Policies



Permissions

Solutions



Catalog



Settings



More resources



Customize navigation



Show all

Solutions



Catalog



Settings



More resources

Compliance Manager

[Overview](#)

[Improvement actions](#)

[Solutions](#)

[Assessments](#)

Compliance Manager measures your progress in completing actions

Overall compliance score

Your compliance score: 75%



14608/19301 points achieved

Your points achieved ⓘ

232/4925

Microsoft managed points achieved ⓘ

14376/14376

Compliance score measures your progress towards completing recommended actions to reduce risks around data protection and regulatory standards.

[Learn how your Compliance score is calculated](#)

Compliance score breakdown

Overall compliance score

Your compliance score is featured prominently at the top. It shows a percentage based on points achievable for completing improvement actions that address key data protection standards and regulations. Points from [Microsoft actions](#), which are managed by Microsoft, also count toward your compliance score.

When you come to Compliance Manager for the first time, your initial score is based on the [Microsoft 365 data protection baseline](#). This baseline assessment, which is available to all organizations, is a set of controls that includes common industry regulations and standards. Compliance Manager scans your existing Microsoft 365 solutions and gives you an initial assessment based on your current privacy and security settings. As you add assessments that are relevant to your organization, your score becomes more meaningful for you.

Learn more: [Understand how your compliance score is calculated.](#)

Key improvement actions

This section lists the top improvement actions you can take right now to make the largest positive impact on your overall compliance score. Select **View all improvement actions** to go to your improvement actions page.

Solutions that affect your score

This section highlights solutions containing improvement actions that can positively impact your score, and the number of outstanding improvement actions in those solutions. Select **View all solutions** to visit your solutions page.

Compliance score breakdown

This section gives you a more detailed view of your score in two different ways:

- **Categories:** shows the percentage of your overall score within data protection categories, such as "protect information" or "manage devices."
- **Assessments:** shows the percentage of your progress in managing assessments for particular compliance and data protection standards, regulations, or laws, such as GDPR or NIST 800-53.

Filtering your dashboard view

You can filter your dashboard view to see only the items related to particular regulations and standards, solutions, type of action, assessment groups, or data protection categories. Filtering your view in this way will also filter the score on your dashboard, showing how many points you've achieved out of total possible points based on your filter criteria.

To apply filters:

1. Select **Filter** on the upper-right side of the dashboard.
2. Select your filter criteria from the **Filters** flyout pane, then select **Apply**.

After you apply a filter, you'll see your score adjusted in real time. The compliance score percentage and breakdown information, and the improvement actions and solutions, now only pertain to data covered by your filter criteria. If you sign out of Compliance Manager, your filtered view remains when you sign back in.

To remove filters:

- At the **Applied filters** heading above your compliance score, select the **X** next to the individual filter you want to remove; or
- Select **Filter** on the upper-right side of your dashboard, then on the **Filters** flyout pane, select **Clear filters**.

Improvement actions page

[Improvement actions](#) are actions managed by your organization. Working with improvement actions helps to centralize your compliance activities and align with data protection regulations and standards. Each improvement action gives detailed implementation guidance and a link to launch you into the appropriate solution. Improvement actions can be assigned to users in your organization to perform implementation and testing work. You can also store documentation, notes, and record status updates within the improvement action.

View your improvement actions

The Compliance Manager dashboard shows your key improvement actions. To view all of your improvement actions, select the **Improvement actions** tab on your dashboard, which brings you to your improvement actions page. You can also select **View all improvement actions** underneath the list of key improvement actions on your dashboard to get to your improvement actions page.

The improvement actions page shows all of the improvement actions that are managed by your organization. Actions that are managed by Microsoft can be viewed within each assessment (learn more about [Microsoft actions](#)).

If you have a long list of actions on your improvement actions page, it may be helpful to filter your view. Select **Filter** at the upper-right corner of the actions list. When the **Filters** flyout pane appears, select your criteria from the available options. You can also customize your view by selecting **Group** in the upper-right corner. From the drop-down menu, select to view by group, solution, category, action type, or status.

The default view for this page does not show improvement actions with a test status of **Passed**. To view actions that have passed testing, check the **Passed** box in the Filters flyout pane. Only actions with a test status of **Passed** count toward your score. Some actions may show a **pending update label**. Learn more about [updates to improvement actions](#).

The improvement actions page shows the following data points for each improvement action:

- **Products:** the product being evaluated.
- **Points achieved:** the number of points achieved out of the total available by completing the action
- **Regulations:** the regulations or standards pertaining to the action
- **Group:** the group to which you assigned the action
- **Solutions:** the solution where you can go to perform the action
- **Assessments:** the assessments that contain the action
- **Categories:** the related data protection category (such as, protect information, manage devices, etc.)
- **Test status:**
 - **None** – no status update recorded
 - **Not assessed** - testing hasn't started
 - **Passed** - implementation successfully tested
 - **Failed low risk** - testing failed, low risk
 - **Failed medium risk** - testing failed, medium risk
 - **Failed high risk** - testing failed, high risk
 - **Out of scope** – the action is not in scope for the assessment and doesn't impact your score
 - **To be detected** - for manual test, indicates an action has been implemented but not tested; for automated test, indicates an action is waiting for automation result
 - **Could not be detected** - automated status can't be determined
 - **Partially tested** – automated scoring that awards partial points

- **Action type:** indicates whether the improvement action is technical, meaning it can be implemented within a solution or product, or non-technical, which would be implemented outside of a technical solution
- **Assigned to:** the person this action has been assigned to, if applicable
- **Testing source:** indicates whether the testing source for the action is manual, automatic, or inherited from a parent

Learn more: [See how to assign and perform work on improvement actions.](#)

Solutions page

The solutions page shows the share of earned and potential points as organized by solution. Viewing your remaining points and improvement actions from this view helps you understand which solutions need more immediate attention.

Find the solutions page by selecting the **Solutions** tab on your Compliance Manager dashboard. You can also select **View all solutions** underneath **Solutions that affect your score** in the upper-right section of your dashboard.

Filtering your solutions view

To filter your view of solutions:

1. Select **Filter** at the top-left corner of your assessments list.
2. On the **Filters** flyout pane, place a check next to the desired criteria (regulations, solutions, action types, groups, categories).
3. Select the **Apply** button. The filter pane will close and you'll see your filtered view.

You can also modify your view to see assessments by group, product, or regulation by selecting the type of grouping from the **Group** drop-down menu above your assessments list.

Taking action from the solution page

The solutions page displays your organization's solutions that are connected to improvement actions. The table lists each solution's contribution to your overall score, the points achieved and possible within that solution, and the remaining number of improvement actions grouped in that solution that can increase your score.

There are two ways you can take action from this screen:

1. On the row of your intended solution, under the **Remaining actions** column, select the hyperlinked number. You'll see a filtered view of the improvement actions screen showing untested improvement actions for that solution.
2. On the row of your intended solution, under the **Open solution** column, select **Open**. You'll see the solution or location in the Microsoft 365 and Office 365 security and compliance centers where you can take the recommended action.

Assessments page

The assessments page lists all the [assessments](#) you set up for your organization. Your compliance score denominator is determined by all your tracked assessments. As you add more assessments, you'll see more improvement actions listed on your improvement actions page, and your compliance score denominator increases.

The **activated templates** counter near the top of the page shows the number of active assessment templates currently in use out of the total number of templates available for your organization to use. See [Template availability and licensing](#) for more information.

The assessments page summarizes key information about each assessment:

- **Assessment:** name of the assessment
- **Status:**
 - **Complete** - all controls have a status of "passed," or at least one is passed and the rest are "out of scope"
 - **Incomplete** - at least one control has a status of "failed"
 - **None** - all controls have not been tested
 - **In progress** - improvement actions have any other status, including "in progress," "partial credit," or "undetected"
- **Assessment progress:** the percentage of the work done toward completion, as measured by the number of controls successfully tested
- **Your improvement actions:** the number of completed actions to satisfy implementation of your controls

- **Microsoft actions:** the number of completed actions to satisfy implementation of Microsoft controls
- **Group:** name of the group the assessment belongs to
- **Product:** associated product, such as Microsoft 365 or another product defined for assessment
- **Regulation:** the regulatory standard, policy, or law that applies to the assessment

Filtering your assessments view

To filter your view of assessments:

1. Select **Filter** at the top-left corner of your assessments list.
2. On the **Filters** flyout pane, check your desired criteria.
3. Select the **Apply** button. The filter pane will close and you will see your filtered view.

You can also modify your view to see assessments by group, product, or regulation by selecting the type of grouping from the **Group** drop-down menu above your assessments list.

Default assessment

By default, you'll see the [Data Protection Baseline](#) assessment on the assessments page. Compliance Manager also provides several pre-built [templates](#) for building assessments.

Assessment templates page

A template is a framework for creating an assessment in Compliance Manager. The assessment templates page displays a list of templates and key details. The list includes templates provided by Compliance Manager as well as any templates your organization has modified or created. You can apply filters to find a template based on certification, product scope, country, industry, and who created it.

The **activated templates** counter near the top of the page shows the number of active assessment templates currently in use out of the total number of templates available for your organization to use. See [Template availability and licensing](#) for more information.

Select a template from its row to bring up its details page, which contains a description of the template and further information about certification, scope, and controls details. From this page you can select the appropriate buttons to create an assessment, export the template data to Excel, or modify the template.

